

# WHEN ANY GROUP OF $N$ ELEMENTS IS CYCLIC? <sup>1</sup>

V. Bragin, Ant. Klyachko and A. Skopenkov <sup>2</sup>

We give a simple proof of the well-known fact: any group of  $n$  elements is cyclic if and only if  $n$  and  $\varphi(n)$  are coprime. This note is accessible for students familiar with permutations and basic number theory. No knowledge of abstract group theory is required; a few necessary notions are introduced in the course of the proof.

## Introduction

We call a *group* a nonempty family  $G$  of transformations (i.e. permutations or rearrangements) of some set, which family is closed with respect to composition and taking inverse transformation (i.e. if  $f, g \in G$ , then  $f \circ g \in G$  and  $f^{-1} \in G$ ). Common term: transformation group. Cf. [A, comment to problem 5].

If a finite group  $G$  contains an element  $g$  such that  $G$  consists of all powers of  $g$  (i.e.  $G = \{g, g^2, \dots, g^n, \dots\}$ ), then group  $G$  is called *cyclic*.

We give a simple proof of the following well-known fact.

**Theorem.** *Any group consisting of  $n$  elements is cyclic if and only if  $n$  and  $\varphi(n)$  are coprime.*

Here  $\varphi(n)$  is the number of positive integers not exceeding  $n$  and coprime to  $n$  (the Euler function).

Note that  $n$  and  $\varphi(n)$  are coprime if and only if in the prime decomposition  $n = p_1 \dots p_k$

(\*) all  $p_i$  are different and

(\*\*)  $p_i$  does not divide  $p_j - 1$  for any  $i$  and  $j$ .

Although we did not find such a proof in the literature, we do not claim any novelty. Although we do not use the Sylow theorems, our argument in the second case below is similar to their proof. We do not use the notion of a quotient group, as opposed to more traditional proofs (see, e.g., [B]). One can understand from [BKKSS] how to invent this proof.

## Proof of the “only if” part.

If  $g$  and  $h$  are transformations of disjoint sets  $M$  and  $N$ , then we can regard them as transformations of  $M \sqcup N$  and hence take their composition.

A cycle  $(a_1, a_2, \dots, a_n)$  is the transformation of a set containing  $a_1, a_2, \dots, a_n$  that carries  $a_n$  to  $a_1$  and  $a_i$  to  $a_{i+1}$  for each  $i < n$ , whereas it carries every other element to itself.

If condition (\*) above is violated, e.g.,  $p_1 = p_2 = p$ , then the following group consists of  $n$  elements and is not cyclic:

$$\left\{ (1, 2, \dots, p)^i \circ (p+1, p+2, \dots, p+\frac{n}{p})^j \mid i = 1, \dots, p, \ j = 1, \dots, \frac{n}{p} \right\}.$$

Assume that condition (\*\*) above is violated, e.g.,  $p_1$  divides  $p_2 - 1$ . Denote by  $\mathbb{Z}_k$  the set of residues modulo  $k$  with the summation and the multiplication operations. Then from the primitive root theorem it follows that there is  $a \in \mathbb{Z}_{p_2}$  for which the powers  $a, a^2, \dots, a^{p_1} = 1$  are different. Denote by  $G_{p_1, p_2}$  the group of transformations  $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$  defined by the formula  $f_{k, l}(x, y) := (a^k x, lx + y)$  for  $k \in \mathbb{Z}_{p_1}$  and  $l \in \mathbb{Z}_{p_2}$ . <sup>3</sup> Then the following group is not cyclic (it is even nonabelian):

$$\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, \ j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}. \quad QED$$

<sup>1</sup>We would like to acknowledge M. Vyalyi, P. Kozhevnikov and K. Kohas for useful discussions.

<sup>2</sup>Supported by Simons-IUM Fellowship

<sup>3</sup>In more advanced notation  $G_{p_1, p_2} := \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, \ l \in \mathbb{Z}_{p_2} \right\}$ .

**Proof of the “if” part.**

Denote by  $|X|$  the number of elements in a set  $X$ . Denote given group by  $G$ .

We use the induction on the number of prime factors of  $|G|$ . If  $|G|$  is a prime, then the “if” part is implied by the following Lagrange Theorem.

The **order**  $\text{ord } a$  of an element  $a$  of a group with the identity element  $e$  is the minimal positive integer  $n$  such that  $a^n = e$ . If the group is finite, it is clear that such  $n$  exists.

**Lagrange Theorem (particular case).** *The number of elements of any finite group is divisible by the order of any its element.*

*Proof.* Denote the group by  $G$ . For each  $x \in G$  consider the set  $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$ . By the definition of order these elements are different. Therefore this set contains  $\text{ord } f$  elements. If  $xf^k = yf^l$ , then  $y = xf^{k-l}$ . Therefore for different  $x$  these sets either coincide or are disjoint. Thus  $|G|$  is divisible by  $\text{ord } f$ . QED

Now suppose that the number of prime factors in  $|G|$  is greater than one. We need the following general version of the Lagrange Theorem.

A **subgroup** of a group  $G$  is a subset of  $G$  that is itself a group.

**Lagrange Theorem.** *The number of elements of any finite group is divisible by the number of elements of any subgroup.*

*Proof.* Denote the group by  $G$  and the subgroup by  $\{h_1, h_2, \dots, h_m\}$ . For each  $x \in G$  consider the set  $\{xh_1, xh_2, \dots, xh_m\}$ . This set contains  $m$  elements. If  $xh_k = yh_l$ , then  $y = xh_k h_l^{-1}$ . Therefore for different  $x$  these sets either coincide or are disjoint. Thus  $|G|$  is divisible by  $m$ . QED

A **maximal subgroup** of a group is a maximal by inclusion subgroup not coinciding with  $G$  and containing more than one element. By the induction hypothesis and the Lagrange Theorem, *each maximal subgroup is cyclic.*

For an element  $f$  of a group  $G$  let  $\langle f \rangle$  be the set of all powers of  $f$  (including zero and negative ones). The element  $f$  is called **generating** for the (cyclic) subgroup  $\langle f \rangle$ .

Suppose to the contrary that the group  $G$  is noncyclic. Then each element is contained in a maximal subgroup.

Elements  $f, g$  of a group  $G$  are **conjugate** in  $G$  if  $g = b^{-1}fb$  for some  $b \in G$ .

**First case:** *generator  $f$  of some maximal subgroup is conjugate only to (some of) its powers.* Take  $h \in G \setminus \langle f \rangle$ . Let  $q$  be the minimal positive integer  $n$  such that  $h^n \in \langle f \rangle$ . Such a  $q$  exists because  $h^{\text{ord } h} \in \langle f \rangle$ .

*Proof that  $|G|$  is divisible by  $q$ .* Let  $\text{ord } h = qt + r$  be division of  $\text{ord } h$  on  $q$  with remainder  $r$ . Then  $h^r = h^{\text{ord } h - qt} \in \langle f \rangle$  and  $0 \leq r < q$ . Hence  $r = 0$  by the minimality of  $q$ . So  $\text{ord } h$  is divisible by  $q$ . Therefore by Lagrange Theorem  $|G|$  is divisible by  $q$ . QED

*Proof that  $fh = hf$ .* Since  $h^{\text{ord } h} \in \langle f \rangle$ , using division with a remainder we obtain that By the condition of the first case  $h^{-1}fh = f^k$  for some  $k \in \mathbb{Z}$ . The inclusion  $h^q \in \langle f \rangle$  implies  $f = h^{-q}fh^q = f^{k^q}$  (here the last equality holds for each  $q$  and is proved by induction on  $q$ ). Therefore  $k^q \equiv 1 \pmod{\text{ord } f}$ . Hence  $k$  and  $\text{ord } f$  are coprime. By conditions (\*), (\*\*) and the Lagrange Theorem  $|G|$  and  $\varphi(\text{ord } f)$  are coprime. Since  $|G|$  is divisible by  $q$ , numbers  $q$  and  $\varphi(\text{ord } f)$  are coprime. So there are integers  $x$  and  $y$  such that  $qx + \varphi(\text{ord } f)y = 1$ . Thus  $k \equiv k^{qx + \varphi(\text{ord } f)y} \equiv 1 \pmod{\text{ord } f}$ . Hence  $fh = hf$ . QED

*Completion of the argument for the first case.* Since  $fh = hf$ , the group  $G$  contains a subgroup

$$\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$$

of  $q \text{ord } f$  elements. Hence by condition (\*) and the Lagrange Theorem  $\text{ord } f$  is coprime to  $q$ . Since  $(fh)^j = f^j h^j$  for each  $j$ , we obtain that  $\text{ord}(fh)$  is divisible both by  $q$  and by  $\text{ord } f$ . Hence  $\text{ord}(fh) = q \text{ord } f$ . Thus  $\text{ord}(fh) = q \text{ord } f$ . Since the subgroup  $\langle f \rangle$  is maximal, we have  $\langle fh \rangle = G$ . Thus  $G$  is cyclic. Contradiction. QED

**Second case:** generator of any maximal subgroup is conjugate not only to its powers.

The **product of subsets**  $X$  and  $Y$  of a group  $G$  is the set of all products  $xy$ , where  $x \in X$  and  $y \in Y$ . If one of these subsets consists of only one element, e.g.,  $Y = \{y\}$ , then we write  $Xy$  instead of  $X\{y\}$ .

(1) Any maximal subgroup  $F$  contains the **center**

$$Z = Z(G) := \{a \in G : ga = ag \text{ for any } g \in G\},$$

i.e., the set of elements commuting with each element of the group.

*Proof of assertion (1).* Otherwise  $FZ$  is a larger commutative subgroup. By the maximality of  $F$  we have  $FZ = G$ . Hence  $G$  is commutative. This contradicts to the assumption of the second case. QED

(2) The intersection of two maximal subgroups equals the center.

*Proof of assertion (2).* A nontrivial element of the intersection commutes with all elements of both subgroups. Hence it commutes with any product of several multiples, each multiple being an element of one of our subgroups. The set of such products is a subgroup. By the maximality of our subgroups this subgroup coincides with the entire group. Therefore the intersection is contained in the center.

Assertion (1) implies the converse inclusion. QED

*Conclusion of the proof of the second case: calculations.* Recall that any element of  $G$  is contained in certain maximal subgroup. By (2) for any *non-central* element such a subgroup is unique. So the group is split into the center and disjoint union of complements of maximal subgroups to the center. The number of elements in such complements are the same for conjugate subgroups. Denote by  $\widehat{F}$  the number of non-central elements of  $G$  in the union of subgroups conjugate to given maximal subgroup  $F$ . Let  $F_1, \dots, F_s$  be a maximal family of pairwise non-conjugate maximal subgroups. Then

$$|G| = |Z| + \sum_{i=1}^s \widehat{F}_i.$$

By the left inequality in the following statement the number of summands is at most one; by the right inequality one summand is also impossible. QED

$$(4) |G|/2 \leq \widehat{F} < |G| - |Z|.$$

*Proof of assertion (4).* A subgroup conjugate to a maximal subgroup is also maximal. (Indeed, if  $g^{-1}Fg \subset F' \subset G$ , then  $F \subset gF'g^{-1} \subset G$ .)

Consider the set

$$N(F) := \{a \in G : Fa = aF\}.$$

Then the number of different subgroups conjugate to  $F$  (including  $F$ ) is  $|G|/|N(F)|$ .

(Indeed, the conjugation by each element of  $G$  takes  $F$  to a conjugate subgroup. If the conjugation by two different elements  $u$  and  $v$  takes the  $F$  to the same subgroup, i.e.,  $u^{-1}Fu = v^{-1}Fv$ , then  $Fuv^{-1} = uv^{-1}F$ . This means that  $uv^{-1} \in N(F)$  or, equivalently,  $u \in N(F)v$ . Conversely, the condition  $u \in N(F)v$  implies  $u^{-1}Fu = v^{-1}Fv$ . Clearly,  $|N(F)v| = |N(F)|$ . Therefore the number of elements of  $G$  conjugation by which takes  $F$  to a given subgroup equals  $|N(F)|$ . Therefore the number of different subgroups conjugate to  $F$  is precisely  $|N(F)|$  times less than  $|G|$ .)

We have  $N(F) = F$ .

(Indeed, it is easy to verify that  $N(F)$  is a subgroup. By the assumption of the second case  $N(F) \neq G$ . Since  $N(F) \supset F$ , the maximality implies that  $N(F) = F$ .)

The three assertions just proved imply that  $\widehat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right)$ .

Since  $|G| > |F|$ , we have  $\widehat{F} < |G| - |Z|$ .

By the assumption of the second case,  $Z \neq F$ . By (1) the center is a subgroup of  $F$ . Hence by the Lagrange theorem  $|Z|$  divides  $|F|$ . Therefore  $\widehat{F} \geq |G|/2$ . QED

### References

- [A] V. I. Arnold, Ordinary Differential Equations, The MIT Press (1978), ISBN 0-262-51018-9.
- [B] Ken Brown, Mathematics 4340, When are all groups of order  $n$  cyclic? Cornell University, March 2009, [http://www.cornell.edu/~kbrown/4340/cyclic\\_only\\_orders.pdf](http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf)
- [BKKSS] D. Baranov, A. Klyachko, K. Kohas, A. Skopenkov and M. Skopenkov, When are all groups of order  $n$  cyclic? <http://olympiads.mccme.ru/lktg/2011/6/index.htm>

КОГДА ЛЮБАЯ ГРУППА ИЗ  $N$  ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ? <sup>1</sup>В. Брагин, Ант. Клячко и А. Скопенков <sup>2</sup>

**Аннотация.** Приводится простое доказательство известного факта: *любая группа из  $n$  элементов является циклической тогда и только тогда, когда  $n$  взаимно просто с  $\phi(n)$* . Для понимания доказательства необходимо знание основ теории чисел (включая теорему Ферма-Эйлера). Знаний по теории групп не требуется: приводятся понятия группы, циклической группы и небольшое количество понятий, необходимых для доказательства.

*...The answers to his questions were things she had never imagined  
and found startling, unwelcome, even painful, altering her beliefs.  
U. K. Le Guin, Dragonfly.*

**Зачем и для кого эта заметка.**

Мы хотели бы привлечь внимание к теории групп достаточно широкого круга людей, включая учителей, руководителей кружков и школьников, серьезно интересующихся математикой. В этой теории есть доступные им результаты-жемчужины. Формулировки таких результатов кратки и используют лишь простейшие определения; доказательства красивы и похожи на решения сложных олимпиадных задач. <sup>3</sup>

Эта заметка предназначена для того, кому понятна и интересна формулировка ниже-приведенной теоремы. Она может быть интересна как читателю, знакомому с основами абстрактной теории групп, так и читателю, не знакомому с ними, но изучавшему перестановки и теорию чисел (и имеющему склонность к задачам классификации). Для понимания доказательства необходимо знание основ теории чисел (включая теорему Ферма-Эйлера). Знаний по теории групп не требуется; небольшое количество необходимых понятий вводятся в процессе доказательства. В частности, наше доказательство не привлекает явно понятия факторгруппы, в отличие от более традиционных доказательств (см., например, [B]).

**Основные определения и примеры.** <sup>4</sup>

Назовем *группой преобразований* непустое семейство  $G$  преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если  $f, g \in G$ , то  $f \circ g \in G$  и  $f^{-1} \in G$ ). <sup>5</sup>

*Циклом*  $(a_1, a_2, \dots, a_n)$  называется перестановка множества, содержащего элементы  $a_1, a_2, \dots, a_n$ , которая переводит  $a_n$  в  $a_1$  и  $a_i$  в  $a_{i+1}$  для любого  $i < n$ , а каждый из остальных элементов переводит в себя.

**Примеры.** (1) Группа  $S_n$  *всех* перестановок  $n$ -элементного множества.

(2) Группа перестановок  $\{\text{id} = (1)(2)(3)(4), (13)(24), (1234), (1432)\}$  множества из четырех элементов.

(3) Группа перестановок  $\{(1, 2, 3, 4, 5, 6, 7, 8)^k\}$ ,  $k = 1, 2, \dots, 8$ , 8-элементного множества.

<sup>1</sup> Благодарим М. Вялого, О. Иванова, П. Кожевникова и К. Кохася и за полезные замечания.

<sup>2</sup> Поддержан грантом фонда Саймонса. Инфо: <http://dfgm.math.msu.su/files/skopenkov/PAPERSCI.pdf>

<sup>3</sup> *Добавление от А. Скопенкова.* Именно с таких жемчужин полезно начинать изучение абстрактной теории групп, на примере их доказательства показывая, как появляются основные ее понятия. См. подробнее [S]. К сожалению, в большей части существующей литературы эти жемчужины скрыты за огромным количеством немотивированного материала, что делает их неинтересными и недоступными.

<sup>4</sup> Это пункт может быть пропущен читателем, знакомым с основами абстрактной теории групп.

<sup>5</sup> *Добавление от А. Скопенкова.* ‘...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде  $f(gh) = (fg)h$ . Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет.’ (В.И. Арнольд, [А, стр. 49, комментарий к задаче 5]). Ср. А. Пуанкаре ‘Наука и метод’, Глава 2 ‘Математические определения и преподавание’ [Р, стр. 455-475], [К].

(4) Группа перестановок  $\{(1, 2, 3)^k(4, 5, 6, 7, 8)^l\}$ ,  $k = 1, 2, 3$ ,  $l = 1, 2, 3, 4, 5$ , 8-элементного множества.

(5) Рассмотрим квадрат на плоскости и все движения плоскости, переводящие его в себя. Это тождественное преобразование, 3 поворота и 4 симметрии. Всего 8 преобразований. Возьмем группу из 8 перестановок множества вершин квадрата, происходящих при применении перечисленных восьми преобразований плоскости.

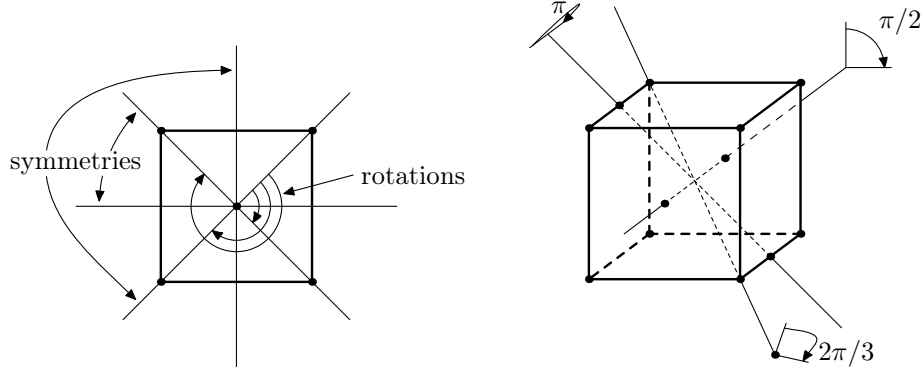


Рисунок: движения квадрата и куба

(6) Рассмотрим куб в пространстве и все вращения пространства (включая тождественное), переводящие его в себя.

(a) Возьмем группу из всех перестановок множества *вершин* куба, происходящих при применении таких вращений.

(b) Возьмем группу из всех перестановок множества *середин ребер* куба, происходящих при применении таких вращений.

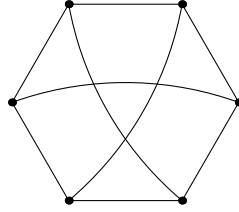


Рисунок: граф  $K_{3,3}$

(7) Группа всех перестановок 6-элементного множества, являющихся изоморфизмами графа  $K_{3,3}$ .

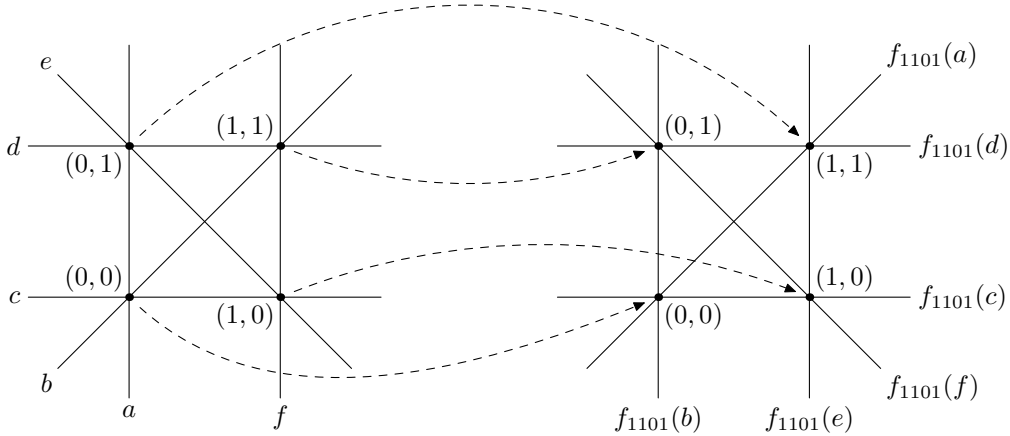


Рисунок: линейное преобразование  $f_{1101} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$

(8) Рассмотрим множество  $\mathbb{Z}_2^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$  упорядоченных пар вычетов по модулю 2. Для любых четырех вычетов  $a, b, c, d$  по модулю 2 рассмотрим отображение  $f_{abcd} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$ , заданное формулой  $f_{abcd}(x, y) = (ax + by, cx + dy)$ . Среди всех таких отображений выберем взаимно-однозначные. Они образуют группу преобразований.

Если в конечной группе преобразований  $G$  найдется преобразование  $g$ , из всех возможных степеней которого состоит  $G$  (т.е.  $G = \{g, g^2, \dots, g^n, \dots\}$ ), то эта группа преобразований называется *циклической*. Например, группы преобразований из примеров (1) для  $n = 2$ , (3) и (4) — циклические, а из остальных примеров — нет.

### Формулировка теоремы.

В этой заметке приводится простое доказательство следующего известного факта.

**Теорема (фольклор).** *Любая группа преобразований из  $n$  элементов является циклической тогда и только тогда, когда  $n$  взаимно просто с  $\phi(n)$ .*<sup>6</sup>

Здесь  $\phi(n)$  — количество целых чисел от 1 до  $n$ , взаимно простых с  $n$  (функция Эйлера).

Заметим, что условие взаимной простоты  $n$  и  $\phi(n)$  равносильно тому, что в разложении числа  $n$  на простые сомножители  $n = p_1 \dots p_t$

(\*) все  $p_i$  различны и

(\*\*)  $p_i$  не делит  $p_j - 1$  ни для каких  $i$  и  $j$ .

Приводимое доказательство не претендует на новизну. Хотя мы не используем теорем Силова, наш разбор второго случая похож на их доказательство. Как его придумать, видно из [BKKSS].

*Почему теорема интересна?* Группы преобразований  $G$  и  $H$  множеств  $M$  и  $N$  называются *изоморфными*, если существует биекция  $\varphi : G \rightarrow H$ , для которой  $\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \circ g_2)$  при любых  $g_1, g_2 \in G$ . Важная тема в математике — классификация групп с точностью до изоморфизма. Ясно, что для любого  $n$  имеется циклическая группа из  $n$  элементов. Поэтому вопрос о *циклическости любой группы из  $n$  элементов* равносильен вопросу о *единственности группы из  $n$  элементов с точностью до изоморфизма*.

### Доказательство части «только тогда»

Обозначим  $\mathbb{Z}/k := \{(1, 2, \dots, k)^i \mid i = 1, 2, \dots, k\}$ .

Если  $g$  и  $h$  — преобразования множеств  $M$  и  $N$ , то преобразование  $g \circ h$  несвязного объединения  $M \sqcup N$  определяется формулой  $(g \circ h)(x) := \begin{cases} g(x) & x \in M \subset M \sqcup N \\ h(x) & x \in N \subset M \sqcup N \end{cases}$ . Для групп  $G$  и  $H$ , состоящих из преобразований множеств  $M$  и  $N$ , определим

$$G \times H := \{g \circ h : M \sqcup N \rightarrow M \sqcup N \mid g \in G, h \in H\}.$$

Если нарушается вышеприведенное условие (\*), например,  $p_1 = p_2 = p$ , то в качестве нециклической группы из  $n$  элементов можно взять группу  $\mathbb{Z}/p \times \mathbb{Z}/\frac{n}{p}$ .<sup>7</sup>

Обозначим через  $\mathbb{Z}_k$  множество вычетов по модулю  $k$  с операциями суммы и произведения, известными из теории чисел. (Не путайте с группой  $\mathbb{Z}/k$ , определенной выше!) Если нарушается вышеприведенное условие (\*\*), например,  $p_1$  делит  $p_2 - 1$ , то *существует вычет  $a \in \mathbb{Z}_{p_2}$ , для которого степени  $a, a^2, \dots, a^{p_1} = 1$  различны*. Это следует из теоремы о первообразном корне (если Вы ее не знаете, примите указанное следствие на веру).

Обозначим через  $G_{p_1, p_2}$  группу преобразований  $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$ , заданных формулой  $f_{k, l}(x, y) := (a^k x, lx + y)$  для  $k \in \mathbb{Z}_{p_1}$  и  $l \in \mathbb{Z}_{p_2}$ .<sup>8</sup> Тогда в качестве нециклической (даже некоммутативной) группы из  $n$  элементов можно взять группу  $G_{p_1, p_2} \times \mathbb{Z}/\frac{n}{p_1 p_2}$ .<sup>9</sup> QED

<sup>6</sup>Ввиду теоремы Кэли в формулировке можно заменить ‘группа преобразований’ на ‘группа’.

<sup>7</sup>Т.е. группу  $\left\{ (1, 2, \dots, p)^i (p+1, p+2, \dots, p+\frac{n}{p})^k \mid i = 1, \dots, p, k = 1, \dots, \frac{n}{p} \right\}$ .

<sup>8</sup> Научно говоря,  $G_{p_1, p_2} = \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, l \in \mathbb{Z}_{p_2} \right\}$ .

<sup>9</sup>Т.е. группу  $\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}$ .

### Доказательство части «тогда».

Через  $|X|$  обозначается число элементов в множестве  $X$ . Обозначим данную группу через  $G$ . Используем индукцию по числу простых сомножителей в  $n = |G|$ . Если сомножитель один, то часть «тогда» вытекает из следующего частного случая теоремы Лагранжа.

**Порядком**  $\text{ord } a$  элемента  $a$  группы с единичным элементом  $e$  называется наименьшее целое положительное  $n$ , для которого  $a^n = e$ . Если группа конечна, то ясно, что такое  $n$  существует.

**Теорема Лагранжа (частный случай).** *Число элементов конечной группы делится на порядок любого ее элемента.*

*Доказательство.*<sup>10</sup> Обозначим данную группу через  $G$ . Для любого  $x \in G$  рассмотрим множество  $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$ . Из определения порядка вытекает, что указанные элементы различны. Значит, в этом множестве  $\text{ord } f$  элементов. Если  $xf^k = yf^l$ , то  $y = xf^{k-l}$ . Поэтому для разных  $x$  эти множества либо не пересекаются, либо совпадают. Значит,  $|G|$  делится на  $\text{ord } f$ . QED

Пусть теперь простых сомножителей в  $n = |G|$  больше одного. Нам понадобится следующая общая версия теоремы Лагранжа.

**Подгруппой** группы называется подмножество этой группы, которое само по себе является группой.

**Теорема Лагранжа.** *Число элементов конечной группы делится на число элементов любой ее подгруппы.*

*Доказательство.* Обозначим данную группу через  $G$ , а ее подгруппу через  $\{h_1, \dots, h_m\}$ . Для любого  $x \in G$  рассмотрим множество  $\{xh_1, xh_2, \dots, xh_m\}$ . В этом множестве  $m$  элементов. Если  $xh_k = yh_l$ , то  $y = xh_k h_l^{-1}$ . Поэтому для разных  $x$  эти множества либо не пересекаются, либо совпадают. Значит,  $|G|$  делится на  $m$ . QED

**Максимальной подгруппой** назовем максимальную по включению подгруппу, не совпадающую со всей группой и содержащую более одного элемента. По предположению индукции и теореме Лагранжа *каждая максимальная подгруппа является циклической*.

Для элемента  $f$  группы  $G$  обозначим через  $\langle f \rangle \subset G$  множество всех его степеней (в т.ч. нулевой и отрицательных). Элемент  $f$  называется **порождающим** для (циклической) подгруппы  $\langle f \rangle$ .

Предположим противное, т.е. что группа  $G$  не является циклической. Тогда *каждый элемент  $f$  содержится в некоторой максимальной подгруппе* (в максимальной по включению подгруппе, содержащей  $\langle f \rangle$ ).

Элементы  $f$  и  $g$  группы  $G$  называются **сопряженными** в  $G$ , если  $g = b^{-1}fb$  для некоторого  $b \in G$ .

**Первый случай:** *порождающий элемент  $f$  некоторой максимальной подгруппы сопряжен только с некоторыми своими степенями.* Возьмем  $h \in G - \langle f \rangle$ . Обозначим через  $q$  наименьшее из целых положительных  $n$ , для которых  $h^n \in \langle f \rangle$ . Такое  $q$  существует, поскольку  $h^{\text{ord } h} \in \langle f \rangle$ .

*Доказательство того, что  $|G|$  делится на  $q$ .* Поделим с остатком  $\text{ord } h$  на  $q$ :  $\text{ord } h = qt + r$ . Тогда  $h^r = h^{\text{ord } h - qt} \in \langle f \rangle$  и  $0 \leq r < q$ . Поэтому ввиду минимальности  $q$  имеем  $r = 0$ . Т.е.  $\text{ord } h$  делится на  $q$ . Значит, по теореме Лагранжа  $|G|$  делится на  $q$ . □

*Доказательство того, что  $hf = fh$ .* По условию первого случая  $h^{-1}fh = f^k$  для некоторого  $k \in \mathbb{Z}$ . Значит,  $f = h^{-q}fh^q = f^{k^q}$  (последнее равенство верно для произвольного  $q$  и доказывается индукцией по  $q$ ). Поэтому  $k^q \equiv 1 \pmod{\text{ord } f}$ . Следовательно,  $k$  и  $\text{ord } f$  взаимно просты. По теореме Лагранжа и условиям (\*) и (\*\*),  $|G|$  и  $\varphi(\text{ord } f)$  взаимно просты. Так как  $|G|$  делится на  $q$ , то  $q$  и  $\varphi(\text{ord } f)$  взаимно просты. Следовательно, найдутся целые  $x$  и  $y$ ,

<sup>10</sup>Более подробно это доказательство (и его обобщение, см. ниже) изложено в [KS, стр. 64].



для которых  $qx + \varphi(\text{ord } f)y = 1$ . Значит,  $k \equiv k^{qx + \varphi(\text{ord } f)y} \equiv 1 \pmod{\text{ord } f}$ . Поэтому  $fh = hf$ . QED

*Завершение разбора первого случая.* Так как  $fh = hf$ , то в  $G$  есть подгруппа

$$\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$$

из  $q \text{ord } f$  элементов. Значит, по условию (\*) и теореме Лагранжа  $\text{ord } f$  и  $q$  взаимно просты. Так как  $(fh)^j = f^j h^j$  для любого  $j$ , то  $\text{ord}(fh)$  делится на  $q$  и на  $\text{ord } f$ . Поэтому  $\text{ord}(fh) = q \text{ord } f$ . Так как подгруппа  $\langle f \rangle$  максимальна, то  $\langle fh \rangle = G$ . Значит,  $G$  циклическая. Противоречие. QED

**Второй случай:** порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.<sup>11</sup>

**Произведением двух подмножеств  $X$  и  $Y$**  группы  $G$  называют множество всевозможных произведений  $xy$ , где  $x \in X$  и  $y \in Y$ . Если одно из этих подмножеств состоит только из одного элемента, например,  $Y = \{y\}$ , то для краткости пишут  $Xy$  вместо  $X\{y\}$ .

(1) Любая максимальная подгруппа  $F$  содержит центр

$$Z = Z(G) := \{a \in G : ga = ag \text{ для любого } g \in G\},$$

т.е. множество тех элементов, которые коммутируют со всеми.

*Доказательство утверждения (1).* Иначе  $FZ$  — большая коммутативная подгруппа, чем  $F$ . Ввиду максимальной  $F$  имеем  $FZ = G$ . Значит,  $G$  коммутативна. Поэтому порождающий элемент любой максимальной подгруппы сопряжен только с собой. Это противоречит условию второго случая. QED

(2) Пересечение двух максимальных подгрупп равно центру.

*Доказательство утверждения (2).* Неединичный элемент в пересечении коммутирует с элементами обеих подгрупп. Значит, он коммутирует с любым произведением нескольких сомножителей, каждый из которых лежит в одной из наших подгрупп. Множество таких произведений является подгруппой, содержащей обе максимальные подгруппы. В силу максимальной наших подгрупп эта подгруппа совпадает со всей группой. Значит, пересечение содержится в центре.

Из (1) вытекает обратное включение. QED

*Завершение разбора второго случая: подсчет.* Напомним, что любой элемент группы содержится в некоторой максимальной подгруппе. Ввиду (2) для любого нецентрального элемента такая подгруппа единственна. Поэтому вся группа разбивается на центр и несвязное объединение дополнений максимальных подгрупп до центра. Количества элементов в таких дополнениях одинаковы для сопряженных максимальных подгрупп. (Подмножества  $F, F' \subset G$  называются сопряженными, если  $g^{-1}Fg = F'$  для некоторого  $g \in G$ .) Обозначим через  $\hat{F}$  общее количество нецентральных элементов во всех максимальных подгруппах, сопряженных с максимальной подгруппой  $F$ . Обозначим через  $F_1, \dots, F_s$  наибольший набор попарно несопряженных максимальных подгрупп. Тогда

$$|G| = |Z| + \sum_{i=1}^s \hat{F}_i.$$

Ввиду левого неравенства в следующем утверждении число слагаемых не превосходит единицы, а ввиду правого — одного слагаемого тоже быть не может. QED

(3)  $|G|/2 \leq \hat{F} < |G| - |Z|$ .

*Доказательство утверждения (3).* Подгруппа, сопряженная к максимальной, также максимальна.

<sup>11</sup>Вот план немного другого разбора второго случая, предложенный М.Н. Вялым. Сначала вводим множество  $N(F)$  из доказательства утверждения (3) ниже. Доказываем, что  $N(F) = F$ , см. там же. Тогда (1) очевидно, так  $Z(G) \subset N(F)$ . Далее делаем то же, что и в приводимом разборе.

(Действительно, если  $g^{-1}Fg \subset F' \subset G$ , то  $F \subset gF'g^{-1} \subset G$ .)

Рассмотрим множество

$$N(F) := \{a \in G : Fa = aF\}.$$

Тогда число различных подгрупп, сопряженных с  $F$  (включая  $F$ ), равно  $|G|/|N(F)|$ .<sup>12</sup>

(Действительно, сопряжение каждым элементом группы  $G$  переводит подгруппу  $F$  в одну из сопряженных подгрупп. Если сопряжение двумя разными элементами  $u, v$  группы  $G$  переводит подгруппу  $F$  в одну и ту же подгруппу, т.е.  $u^{-1}Fu = v^{-1}Fv$ , то  $(uv^{-1})^{-1}Fuv^{-1} = F$ . Это означает, что  $uv^{-1} \in N(F)$  или, что то же самое,  $u \in N(F)v$ . Обратно, условие  $u \in N(F)v$  влечет  $u^{-1}Fu = v^{-1}Fv$ . Ясно, что  $|N(F)v| = |N(F)|$ . Поэтому число элементов в  $G$ , сопряжение с которыми переводит подгруппу  $F$  в данную фиксированную сопряженную подгруппу, равно  $|N(F)|$ . Значит, число подгрупп, сопряженных к  $F$ , равно в  $|N(F)|$  раз меньше, чем элементов группы  $G$ .)

Имеем  $N(F) = F$ .

(Действительно,  $N(F)$  является подгруппой. По условию второго случая  $N(F) \neq G$ . Так как  $N(F) \supset F$ , то в силу максимальной  $N(F) = F$ .)

$$\text{Ввиду трех доказанных утверждений } \widehat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right).$$

Так как  $|G| > |F|$ , то  $\widehat{F} < |G| - |Z|$ .

По (1) центр является подгруппой в  $F$ . Значит, по теореме Лагранжа  $|Z|$  делит  $|F|$ . По условию второго случая  $Z \neq F$ . Следовательно,  $|Z| \leq |F|/2$ . Поэтому  $\widehat{F} \geq |G|/2$ . QED

### Литература

- [A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.
- [B] Ken Brown, Mathematics 4340, When are all groups of order  $n$  cyclic? Cornell University, March 2009, [http://www.cornell.edu/~kbrown/4340/cyclic\\_only\\_orders.pdf](http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf)
- [BKKSS] Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков, Когда любая группа из  $n$  элементов циклическая? <http://olympiads.mccme.ru/lktg/2011/6/index.htm>
- [K] Ф. Клейн, Элементарная математика с точки зрения высшей.
- [KS] Л.А. Калужнин и В.И. Суцанский, Преобразования и перестановки, М.: Наука, 1985.
- [P] А. Пуанкаре, О науке, М.: Наука, 1990.
- [S] А. Скопенков, Философски-методическое отступление, в кн. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова, Москва, МЦНМО, 2009. <http://www.mccme.ru/circles/oim/mvz.pdf> (засмотрено 20.08.2011).

<sup>12</sup>Это вытекает из теоремы о длине орбиты для действия группы на себе сопряжениями. Те, кому это доказательство непонятно, могут прочитать следующий абзац.